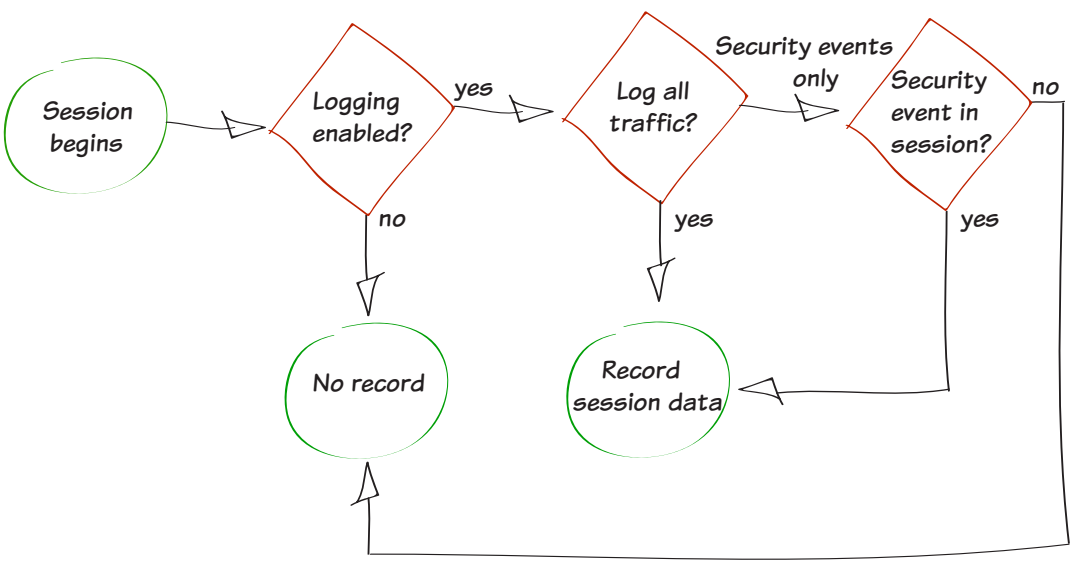
Logging network traffic to gather information

This example demonstrates how to enable logging to capture the details of the network traffic processed by your FortiGate unit. Capturing log details will provide you with detailed traffic information that you can use to asses any network issues.

1. Recording log messages and enabling event logging
2. Enabling logging in the security policies
3. Results



1. Recording log messages and enabling event logging

Go to **Log & Report > Log Config > Log Settings**.

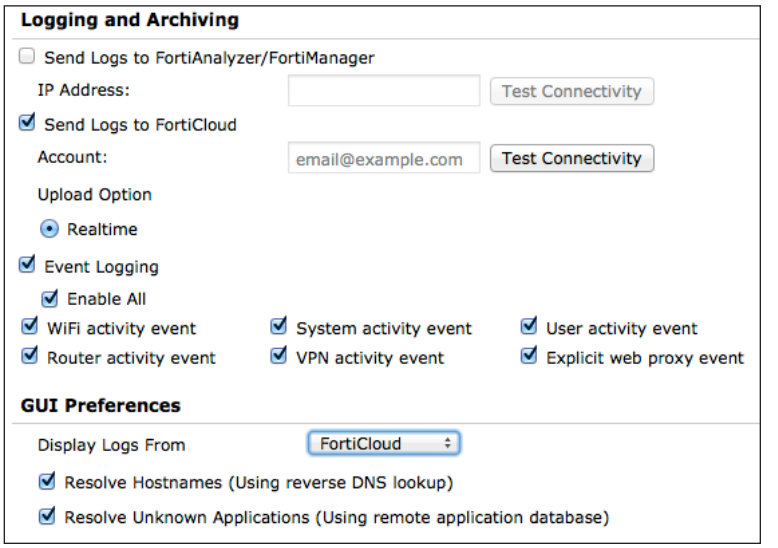
Select where log messages will be recorded. You can save log messages to disk if it is supported by your FortiGate unit, to a FortiAnalyzer or FortiManager unit if you have one, or to FortiCloud if you have a subscription. Each of these options allow you to record and view log messages and to create reports based on them.

In most cases, it is recommended to **Send Logs to FortiCloud**, as shown in the example.

Next, enable **Event Logging**.

You can choose to **Enable All** types of logging, or specific types, such as **WiFi activity events**, depending on your needs.

Under the **GUI Preferences** ensure that the **Display Logs From** is set to the same location where the log messages are recorded (in the example **FortiCloud**).

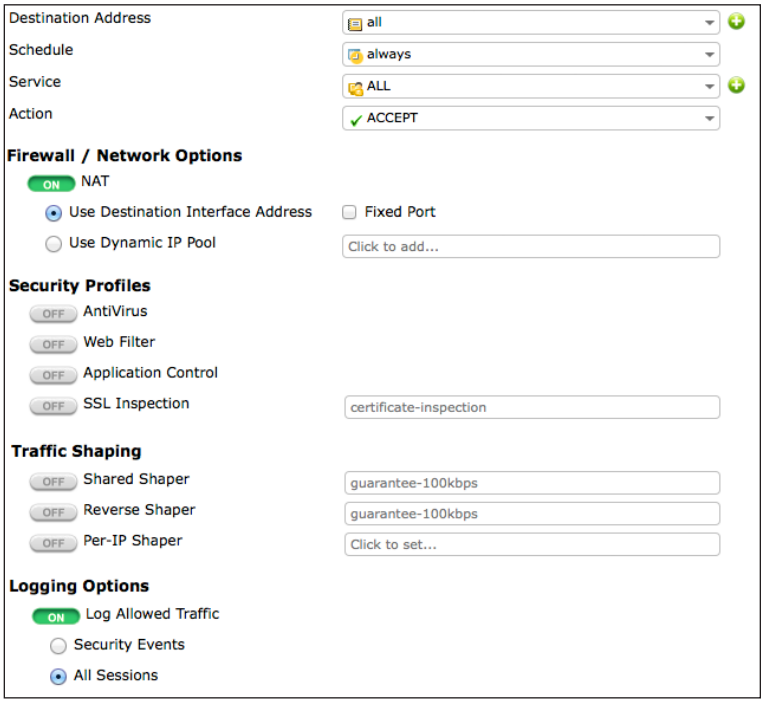


2. Enabling logging in the security policies

Go to **Policy & Objects > Policy > IPV4**. Edit the policies controlling the traffic you wish to log.

Under **Logging Options**, select either **Security Events** or **All Sessions**.

In most cases, you should select Security Events. All Sessions provides detailed traffic analysis but also but requires more system resources and storage space.



3. Results

View traffic logs by going to **Log & Report > Traffic Log > Forward Traffic**. The logs display a variety of information about your traffic, including date/time, source, device, and destination.

To change the information shown, right-click on any column title and select **Column Settings** to enable or disable different columns.

Date/Time	Src	Device	Dst
10:23:02	192.168.1.117	00:0c:29:c2:38:8e	208.91.113.70
10:22:23	192.168.1.117	00:0c:29:c2:38:8e	208.91.112.53
10:22:02	192.168.1.100	00:09:0f:7e:71:fe	208.91.113.184
10:20:03	192.168.1.100	00:09:0f:7e:71:fe	208.91.112.53
10:18:58	192.168.1.117	00:0c:29:c2:38:8e	208.91.112.50
10:18:51	192.168.1.100	00:09:0f:7e:71:fe	208.91.113.184
10:15:43	192.168.1.100	00:09:0f:7e:71:fe	208.91.113.184
10:13:44	192.168.1.100	00:09:0f:7e:71:fe	208.91.112.53
10:12:54	192.168.1.117	00:0c:29:c2:38:8e	208.91.113.70
10:12:32	192.168.1.100	00:09:0f:7e:71:fe	208.91.113.184